What is claimed is:

1. A method for on-connect security scan and delivery, comprising:

interfacing with a remote access infrastructure to detain a client in a virtual lobby when the client attempts to connect to a network;

scanning the client to determine if the client complies with security requirements; and

permitting connection to the network only if the client complies with the security requirements.

2. The method as recited in claim 1, further comprising:

interfacing with at least one provider of at least one security mechanism to bring the client into compliance with the security requirements, if the client is not in compliance.

3. The method as recited in claim 1, further comprising:

retrieving client information from a repository.

4. The method as recited in claim 1, further comprising:

performing a security risk assessment for the network; and

creating the security requirements to address risks identified in the security risk assessment.

5. The method as recited in claim 4, further comprising:

storing the security requirements in a repository.

6. The method as recited in claim 4, further comprising:

updating the security requirements with a new policy; and

interfacing with at least one provider to provide delivery of at least one security mechanism to at least partly implement the new policy.

7. The method as recited in claim 6, further comprising:
certifying the at least one provider.

8. The method as recited in claim 6, further comprising:
storing the new policy in a repository.

9. The method as recited in claim 6, further comprising:
providing a custom configuration tool to at least partly implement the new policy.

10. A network security authority system, comprising:
a computing system in a virtual lobby between an inner firewall protecting a network and an outer firewall protecting the virtual lobby;
a software component operable on the computing system to prevent an insecure connection between a client and the network by scanning the client to determine if the client complies with security requirements.

11. The network security authority system as recited in claim 10, wherein, if scanning reveals non-compliance, the software component provides at least one security mechanism to the client so that the client complies with the security requirements before permitting the client to connect to the network.

12. The network security authority system as recited in claim 10, further comprising:
a remote access infrastructure to interface with the software component.

13. The network security authority system as recited in claim 12, wherein the remote access infrastructure processes at least dialup and virtual private network (VPN) connections.

14. A method for on-connect security scan and delivery, comprising:
controlling configuration of a plurality of security mechanisms for a

client based on security requirements for a network;

scanning the client for an indication of whether the client complies with the security requirements;

providing a delivery assistant to the client to install and configure at least one of the plurality of security mechanisms; and

permitting connection to the client, only if the client complies with the security requirements.

15. The method as recited in claim 14, further comprising:

certifying third-party security mechanisms that meet the security requirements; and

distributing the certified third-party security mechanisms to the client through the delivery assistant.

16. The method as recited in claim 14, further comprising:

storing client information, delivery information, and security requirements in a repository.

17. The method as recited in claim 14, further comprising:

providing an optional delivery to the client.

18. The method as recited in claim 14, further comprising:

presenting a security warning to the client.

19. The method as recited in claim 18, further comprising:

scheduling a future delivery for the client.

20. A network security authority system, comprising:

a virtual lobby computing system in communication with two firewalls to protect a network from insecure clients attempting to connect to the network;

a scanning component operable on the computing system to determine if a client complies with security requirements and to determine if lacking security

mechanisms are available for delivery; and

a delivery component operable on the computing system to deliver available security mechanisms to the client.

21. The network security authority system as recited in claim 20, further comprising:

a repository component in communication with the computing system to store the security requirements.

22. The network security authority system as recited in claim 21, wherein the repository component is a database management system.

23. The network security authority system as recited in claim 22, wherein the repository component operates to manage the security requirements and associated delivery instructions for available security mechanisms.

24. The network security authority system as recited in claim 20, further comprising:

a certification system in communication with the computing system to certify third-party security mechanisms that meet the security requirements.

25. An article of manufacture having instructions stored on it that cause a computing system to operate as a network security authority, the instructions comprising:

detaining a client that is attempting to connect to a network in a virtual lobby, the virtual lobby being between an outer firewall and an inner firewall, the inner firewall being between the virtual lobby and the network;

providing resources for scanning the client to verify the client complies with security requirements;

providing implementation resources to help the client to comply with security requirements; and

denying permission for the client to connect to the network upon

determining that the client does not comply with security requirements and that the implementation resources to bring the client into compliance are not available.

26. The instructions as recited in claim 25, further comprising:

providing warnings for select security requirements and permitting the client to connect to the network; and

enforcing rules for overriding the select security requirements;

wherein the rules for overriding are adaptably defined under the circumstances.

27. The instructions as recited in claim 25, further comprising:

scheduling later operations to bring the client into compliance for select security requirements.

28. The instructions as recited in claim 25, further comprising:

providing a presentation notifying the client of scanning.

29. The instructions as recited in claim 25, further comprising:

providing a presentation of implementation resources information to the client.

30. The instructions as recited in claim 25, further comprising:

providing a presentation of a compliance status to the client.

31. A network security authority system, comprising:

a network;

an inner firewall to prevent unauthorized access to the network;

a virtual lobby to determine if a client complies with security requirements;

an outer firewall to prevent unauthorized access to the virtual lobby;

a computing system in communication with the virtual lobby; and

a software component operable on the computing system in the virtual lobby to determine if the client complies with the security requirements and to provide delivery of any security mechanisms required for the client to comply with the security requirements, before allowing the client access to the network inside the inner firewall.

32. The system as recited in claim 31, wherein the software component comprises:

a scanning component operable on the computing system to scan a client for security mechanisms complying with the security requirements, when the client attempts to connect to the computing system;

a delivery component operable on the computing system to provide deliveries to the client to comply with the security configuration; and

a repository component operable on the computing system and having repository tools accessible by the scanning component and the delivery component, the repository component to hold the security requirements, and delivery information.

33. The system as recited in claim 32, wherein the repository component also holds security policy information.

34. The system as recited in claim 33, wherein the repository component comprises a policy management system.

35. A method of doing business, comprising:

providing a software product to an enterprise configured to scan clients attempting to connect to a network and to provide delivery of security mechanisms to comply with security requirements;

updating security requirements in the software product; and

integrating delivery of new security mechanisms into the software product when the security requirements are updated.

36. The method of doing business as recited in claim 35, wherein providing delivery of security mechanisms comprises providing webpages for downloading.

37. The method of doing business as recited in claim 35, wherein the delivery of security mechanisms is semi-automatically integrated into the software product.

38. The method of doing business as recited in claim 35, further comprising:
eliminating a security mechanism from the software product when it is no longer needed to comply with the security requirements.

39. The method of doing business as recited in claim 35, further comprising:
contracting with a vendor to provide delivery of at least one security mechanism.

40. The method of doing business as recited in claim 39, further comprising:
tracking revenue generated from deliveries to the client over time and delivering at least a percentage of the revenue to the enterprise.

41. The method of doing business as recited in claim 39, further comprising:
tracking revenue generated from deliveries by the vendor over time and delivering at least a percentage of the revenue to the enterprise.

42. The method of doing business as recited in claim 39, wherein the at least one security mechanism is an anti-virus software product.